SUBJECT:

General Overview

This section addresses the specific accounting, reporting, and budgeting conventions that Minnesota counties should use. It details the mandatory procedures for all counties and those that, while not mandatory, are desirable practices which counties should adopt.

COFARS addresses generally accepted accounting principles for local government. It has modified suggested implementation of these principles to allow counties to account during the year on a cash basis and convert to the modified accrual basis and accrual basis for year-end reporting.

Since the time when the original COFARS manual was released, Minnesota counties have generally modified their accounting methods to conform to the mandatory procedures. This issue of COFARS is based on the new governmental financial reporting model established by the Governmental Accounting Standards Board in Statement No. 34, *Basic Financial Statements--and Management's Discussion and Analysis--for State and Local Governments.*

This Page Intended To Be Blank

SUBJECT:

Internal Control

PURPOSE:

This section contains the internal control standards to be followed by counties in establishing and maintaining systems of internal control.

PRINCIPLES:

Internal control systems are to reasonably ensure that the following objectives are achieved:

- Expenditures and commitments comply with applicable law.
- Assets are safeguarded against waste, loss, unauthorized use, and misappropriation.
- Transactions are recorded properly so that reliable financial and statistical reports can be prepared and accountability for assets is maintained.

The following concept of internal control is useful in understanding and applying the internal control standards set forth and discussed on succeeding pages:

> An internal control system consists of the plan of organization and methods and procedures adopted by management to ensure that resource use is consistent with laws, regulations, and policies; that resources are safeguarded against waste, loss, and misuse; and that reliable data are obtained, maintained, and fairly disclosed in financial statements.

The ultimate responsibility for good internal controls rests with management. Internal controls should not be looked upon as separate, specialized systems. Rather, they should be recognized as an integral part of each system that management uses to regulate and guide its operations. In order to ensure the proper conduct of government business, management must periodically review its internal control systems. This review should be sufficient in scope to provide the answers to several basic questions:

- C Are the systems we have in place adequate to manage and account for our resources, meet our goals and objectives, and ensure compliance with state and federal regulations?

- C Is there an audit trail from our reports to our source documents, or will we have to rely on someone to "remember" the facts?

- C Are all our departments properly using the systems we have in place, and are they complying with our internal policies and procedures?

- C Have we strengthened our system of internal control by segregating duties among our employees to provide cross-checks and by providing for the physical security of our assets (e.g., official prenumbered receipts, locking cash drawers, regular inventories, etc.) to the maximum extent practicable?

These are the broad questions your auditor will also seek to answer through the course of his or her audit. If you are satisfied with the results of your review, then there is a much greater likelihood that your auditor will also be satisfied. If you identify problem areas, then you have an opportunity to discuss them with your auditor and to correct them before the auditor is obliged to comment on the problems in his or her report.

SUBJECT:

Internal Control Structure

PRINCIPLES:

This section provides guidance on internal control policies that are based on the 1994 report issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and standards adopted by the American Institute of Certified Public Accountants and the Federal Office of Management and Budget.

Internal control is defined in the COSO report as follows:

> Internal control is a process affected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
>
> - Effectiveness and efficiency of operations
> - Reliability of financial reporting
> - Compliance with applicable laws and regulations

What does this mean for counties?

Internal control is a management process for keeping an entity on course in achieving its business objectives as adopted by the governing body. This management control system should ensure that resources are guarded against waste, loss, and misuse; that reliable data is obtained, maintained, and fairly disclosed in financial statements and other reports; and resource use is consistent with laws, regulations, and policies.

Basic Internal Control Requirements

Each county is responsible for establishing and maintaining a collective system of internal control throughout their government.

An internal control system should provide *reasonable assurance* that an entity will accomplish its objectives. The concept of reasonable assurance recognizes that the cost of an internal control activity should not exceed the benefit derived from it. Reasonable assurance equates to a satisfactory level of confidence given considerations of costs, benefits, and risks.

The county's management must identify and analyze their own risks to determine how those risks should be managed. Management defines the level of risk that the entity is willing to accept and strives to maintain risks within those levels.

Each entity should adopt methods to assess risk and review control activities. The methods developed should address each entity's own specific needs.

Components of Internal Controls

The five components of good internal controls within a management control system are:

1. **Control Environment** - The control environment sets the tone of an entity. It influences the control consciousness of its people and it is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, and competence of the entity's staff; management's philosophy and operating style; the way management assigns authority and responsibility; the way management organizes and develops its staff; and the attention and direction provided by the board.

2. **Risk Assessment** - Every entity faces a variety of risks from external and internal sources, all of which must be assessed. Risk assessment is the identification and analysis of relevant risks to achieving the objectives and forms a basis for determining how risks should be managed. Because economic, regulatory, and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change.

3. **Control Activities** - Control activities are the internal policies and procedures that help ensure management directives are carried out. They help ensure necessary actions are taken to address risks to achieving the government's objectives. Control activities occur throughout the organization at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, review of operating performance, security of assets, and segregation of duties.

4. **Information and Communication** - Pertinent information must be identified, captured, and communicated in a form and time frame that enables people to carry out their responsibilities. Information systems produce reports containing operational, financial, and compliance-related information, making it possible to run and control the entity.

   Effective communication is also essential with external parties, such as taxpayers, vendors, legislators, and other interested parties.

5. **Monitoring** - Management systems and internal activities need to be monitored to assess the quality of their performance over time. Assessment is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two. Ongoing monitoring occurs in the course of operations, including regular management and supervisory activities and other action personnel take in performing their duties. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Deficiencies should be reported upstream, with serious matters reported to top management.

Common Questions About Internal Control

What is a risk assessment?

A risk assessment is an ongoing process to identify, analyze, and manage risk. An entity needs a plan to identify both external and internal risks. The plan will help management understand how those risks affect their activities, assess their significance, manage their effect, and provide for continuous monitoring. The following are some examples of external and internal risks:

- External risks arise from activities outside the entity. Technological developments, changing public expectations, legislative directives, natural catastrophes, and economic changes all have the potential for creating external risks in an entity.

- Internal risks are less predictable and arise from activities inside the entity. Disruption of the computer systems or telephone systems causes obvious operational problems. When new managers are hired, changes in management style can affect internal control objectives.

How do you identify risk?

Identification of risks can start from existing systems. The budget process, audits, strategic planning, and other chapters included in this manual all provide opportunities for managers to conduct quantitative and qualitative reviews and to identify and prioritize. More informal opportunities include management planning meetings, meetings with an auditor, and everyday interaction with staff.

More important than the specific method used to identify risks is management's careful consideration of factors unique to the entity. Some key factors, such as an entity's past experience in failing to meet objectives, staff quality, statutory framework, or the significance and complexity of activities in relation to the entity's mission, should receive management's careful consideration.

By analyzing organizational activities, managers apply risk assessment to functions. Successfully managing risk at the activity level is vital to maintaining an acceptable level of risk for the organization.

What is risk analysis?

Risk analysis involves a careful, rational process of estimating the significance of a risk, assessing the likelihood of its occurrence, and considering what actions and controls need to be taken to manage it. Risk analysis also involves estimating the cost to the entity if something does go wrong. That analysis is based on the entity's assumptions about the risk and costs associated with reducing it. Sometimes an actual risk may appear to require one set of actions, but the perceived risk, coupled with media reaction to that risk, requires a more expensive set of actions.

It is also important to recognize the distinction between risk assessment (a part of a management control system) and actually managing risk (part of an organization's operations). Limitations on resources will define the level to which risks can be managed.

How do you control or minimize risk?

The control of risk starts with management deciding on the actions necessary to reduce the potential occurrence and significance of loss and the monitoring conditions needed to remain aware of changing circumstances. Management tools for an early warning system include information systems and ensuring appropriate data is captured, processed, and reported.

If an entity builds its components of a management control system into its planning efforts, as well as its daily activities, it is more likely to avoid unnecessary costs, make quick responses as needs arise, and adapt to decreasing resources and changing political and economic climates.

Do control activities increase staffing requirements?

Although control activity procedures are not intended to increase staffing levels, acceptable procedures are to be established and followed which may require changes in existing workloads and/or additional staff position(s). However, a periodic thorough internal review of control activities may identify policies and procedures that are no longer required. It is recognized that some small to medium entities may not be able to institute internal controls on the same level as larger, more complex entities. In those cases where staffing may prohibit or restrict the appropriate segregation of duties, management must either have more active oversight of operations or utilize personnel from other organizational units to the extent possible as compensating controls.

More About Control Activities

The control activities presented in this section are intended to provide management and other staff with an overview on the use and potential limitations of control activities to manage the risk of achieving the entity's objectives.

Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to the achievement of an entity's objectives. Control activities occur throughout the entity at all levels and in all functions.

Control activities are actions taken to minimize risk. The need for a control activity is established in the risk assessment process. When the assessment has identified a significant risk to the achievement of an objective, a corresponding control activity should be determined. If control activities are in place for each significant operation, and if management makes sure those activities are carried out properly, staff can be reasonably confident the management control system will provide the necessary assurances.

Control activities and procedures should be considered to ensure the entity is in compliance with contracts, agreements, laws, and regulations applicable to counties. Generally, those activities and procedures may be categorized into one of the following areas and completed by personnel at various levels:

- **Top-level performance reviews** - Performance reviews should be made of actual performance versus budgets, forecasts, and performance in prior periods. Major initiatives should be tracked and management actions taken to analyze and follow up where appropriate.

- **Direct functional or activity management reviews** - Performance reviews should be made of specific functions or activities. The reviews may focus on compliance, financial, or operational issues.

- **Informational processing** - A variety of control activities should be performed to check the accuracy and completeness of information as well as the authorization of transactions. Development of new systems and changes to existing ones should be controlled. Additionally, access to programs and data should be restricted.

- **Physical controls** - Equipment, inventories, cash, and other assets should be secured physically and periodically counted and compared with amounts shown on control records.

- **Performance indicators** - Certain operating results can be anticipated. By investigating unexpected results or unusual trends, circumstances that jeopardize the achievement of objectives can be identified.

- **Segregation of duties** - Duties are divided, or segregated, among different people to reduce the risk of error or inappropriate actions. For example, responsibilities for authorizing transactions, recording them, and handling the related assets should be separated.

What are some potential limitations of control activities?

Control activities, no matter how well designed and executed, can provide only reasonable assurance regarding achievement of objectives. The likelihood of achievement is affected by limitations inherent in all control systems. These limitations include the following:

- **Judgment** - The effectiveness of controls will be limited by the fact that decisions must be made with human judgment in the time available, based on information at hand, and under the pressures to conduct business.

- **Breakdowns** - Even if control activities are well designed, they can break down. Personnel may misunderstand instructions or simply make mistakes. Errors may also stem from new technology and the complexity of computerized information systems.

- **Management override** - Even in effectively controlled organizations, high level personnel may be able to override prescribed policies or procedures for personal gain or advantage. This should not be confused with management intervention, which represents management actions to depart from prescribed policies or procedures for legitimate purposes.

- **Collusion** - Complicity between two or more individuals can result in control failures. Individuals acting collectively often can alter financial data or other management information in a manner that cannot be identified by the control system.

- **Cost vs. benefit** - In determining whether a particular control activity should be established, the risk of failure and the potential effect must be considered along with the cost of establishing the control. Excessive control is costly and counterproductive. Too little control presents undue risk. Entities should make a conscious effort to strike an appropriate balance.

This Page Intended To Be Blank